Release Notes

For Red Hat Certificate System Errata RHSA-2009:0007

Copyright © 2009 Red Hat, Inc.

Copyright © 2009 Red Hat, Inc.. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later with the restrictions noted below (the latest version of the OPL is presently available at *http://www.opencontent.org/openpub/*).

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive
Raleigh, NC 27606-2072USAPhone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588Research Triangle Park, NC 27709USA

1. Important Changes for Red Hat Certificate System 7.3 Errata Update 2
    1.1. Port Separation 2
    1.2. New LDAP Publishing Password Parameter 5
    1.3. Added Support for Using Internet Explorer on Windows Vista 5
2. Known Issues in Errata RHSA-2009:0007 5
3. Bugs Fixed in Errata RHSA-2009:0007 6
4. Platform Support 7
    4.1. Server Support 7
    4.2. Client Support 9
    4.3. Other Required Software 9
    4.4. Optional Server Hardware 10
    4.5. Optional Client Hardware 10
5. Installation and Deployment Notes 10
    5.1. Obtaining Packages 10
    5.2. Installation Notes 10
    5.3. Required JRE 11
    5.4. Required JDK 11
    5.5. TPS Subsystem Considerations 12

5.6. Directory Server Information 12
5.7. Source RPMs 12
6. Copyright and Third-Party Acknowledgments 12

These release notes contain important changes and updates that are specific to Red Hat Certificate System 7.3 Errata RHSA-2009:0007. Information about the default release of Red Hat Certificate System 7.3 is addressed in the standard release notes for the 7.3 release, as well as in the official documentation set for Red Hat Certificate System 7.3.

1. Important Changes for Red Hat Certificate System 7.3 Errata Update

Along with security bug fixes and enhancements applied with Errata RHSA-2009:0007, there are some important changes to the way that some common certificate management tasks.

1.1. Port Separation

For security reasons, some deployments require different TCP ports for the different subsystem interfaces (administrative, agent, and end-entities). Errata RHSA-2009:0007 re-introduces port separation as a configuration option.

Only the subsystems which have separate services interfaces (CA, OCSP, DRM, and TKS) can be configured for port separation. The other subsystems (RA and TPS) cannot.

The port separation is only for *secure* ports. There is still only a single unsecure port.

There are two ways to configure port separation for Certificate System 7.3 subsystems. Existing instances can be edited to have separate service ports, while new instances can be created with separate ports.

1.1.1. Configuring Port Separation for Existing Instances

1. Open the directory instance. For example:

```
cd /var/lib/rhpki-ca/
```

2. Open the configuration directory.

```
cd conf/
```

3. Edit the **`server.xml`** file.

```
vim server.xml
```

4. By default, there is one service defined, between the **<Service>** and **</Service>** tags.

   Copy the default **<Service>** entry. Use the default for the agent service entry, and then paste the default entry twice to add new entries for the admin and end-entities services.

5. In the two new entries, edit the **<Connector port="..."** line with the TCP port and the **<Host appBase="..."** entry to identify the location of the web directory for the service. The **appBase** directory should be something like **webapps.admin** and located in the subsystem's instance directory.

   For example, this creates the admin entry:

```
  <Service name="CatalinaAdmin">

    <Connector port="9445" />

    <Engine name="CatalinaAdmin" defaultHost="localhost">

      <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
             resourceName="UserDatabase"/>

      <Host name="localhost" appBase="webapps.admin"
       unpackWARs="true" autoDeploy="false"
       xmlValidation="false" xmlNamespaceAware="false">

        <Valve className="org.apache.catalina.valves.AccessLogValve"
                 directory="logs"  prefix="localhost_access_log." suf\
fix=".txt"
                 pattern="common" resolveHosts="false"/>

      </Host>

    </Engine>

  </Service>
```

   Edit the end-entities entry similarly as the admin entry.

6. Go up into the instance directory, **/var/lib/rhpki-ca**.

```
cd ../
```

7. Copy the **webapps/** directory for the separate services to use.

```
cp -r webapps webapps.ee
cp -r webapps webapps.admin
```

8. Each web directory contains templates for the three services pages: **agent**, **admin**, and **ee**. For each directory, move the two unused templates so they cannot be accessed. For example, this

moves the **agent** and **admin** templates in the **ee** directory:

```
cd webapps.ee
mv agent agent.orig
mv admin admin.orig
```

Do this for all three services.

9. Still in the **webapps.ee/** directory, open the **WEB-INF** directory.

```
cd WEB-INF/
```

10. Edit the **web.xml** file and comment out the **caauths** servlet mapping.

```
<!--   <servlet-mapping>
      <servlet-name>  caauths  </servlet-name>
      <url-pattern>   /auths  </url-pattern>
   </servlet-mapping>
-->
```

Do this for the agent and end-entities services, but *not* for the administrative service. The admin service has to be able to access the **caauths** admin interface.

11. Open the **lib/** directory and move the **osutil.jar** file so that the common version, not the local version, is used by the service.

```
cd lib/
mv osutil.jar osutil.jar.orig
```

Do this for all three services.

12. Move the **osutil.jar** symlink from **common/lib/** to the **shared/lib/** directory.

```
cd  /var/lib/pki-ca/shared/lib
cp -d /var/lib/pki-ca/common/lib/osutil.jar .
rm /var/lib/pki-ca/common/lib/osutil.jar
```

13. Restart the subsystem.

```
/etc/init.d/rhpki-ca restart
```

1.1.2. Creating New Instances with Separate Ports

New instances can be created automatically with port separation by running the **pkicreate** command with parameters which create separate ports for each service. For example:

```
pkicreate -pki_instance_root=/var/lib -pki_instance_name=pki-ca1 -
agent_secure_port=9543 -ee_secure_port=9544 -admin_secure_port=9545 -
unsecure_port=9180 -tomcat_server_port=1801 -user=pkiuser -group=pkiuser
```

Port separation is optional. To create an instance with a single secure port, simply use the `-secure_port` with **pkicreate**, as before. All of the default instances are still automatically created with a single secure port.

1.2. New LDAP Publishing Password Parameter

In Red Hat Certificate System 7.1 and older versions, passwords were stored in a special cache database. This database was removed in Red Hat Certificate System 7.2 and replaced with a **password.conf** file. However, the LDAP publishing jobs were still configured to store their passwords in the password cache. As long as the LDAP publishing password was the same as the internal database (the related LDAP directory), then the publishing account could connect properly to the directory. If the LDAP publishing password was changed to something other than the internal database password and the CA was restarted, then publishing would fail.

A new password parameter, *ca.publish.ldappublish.ldap.ldapauth.bindPWPrompt*, has been added to the Certificate Manager's **CS.cfg** file. This sets the name of the parameter to use to store the LDAP publishing password in the **password.conf** file. The default setting is as follows:

```
ca.publish.ldappublish.ldap.ldapauth.bindPWPrompt: CA LDAP Publishing
```

When a new password is set for LDAP publishing, it is stored in the **password.conf** file as:

```
CA LDAP Publishing:password
```

1.3. Added Support for Using Internet Explorer on Windows Vista

In Red Hat Certificate System 7.3, the end-entities pages for the subsystems could only be access using Internet Explorer on Windows XP. The certificate processing library on XP is **xenroll.dll**, which was the library used by the subsystem's HTML pages. In Vista, these functions are performed with **certenroll.dll**. This errata adds support for Vista's **certenroll.dll** library so that users can access the end-entities pages on Vista.

2. Known Issues in Errata RHSA-2009:0007

There is a problem with the **pkiconsole** script on Solaris. The Solaris console packages are initially installed using the following command:

```
pkgadd RHATrhpki-managex

rhpki-install -pki_subsystem=all -pki_package_path=location -force
```

At installation, the product variable is improperly set in the **pkiconsole** script. The line reads:

```
PRODUCT=[PKI_PRODUCT]
```

Edit it and change it to the proper product name, **rhpki**:

```
vim /usr/bin/pkiconsole

PRODUCT=rhpki
```

This is Bugzilla #481447.

3. Bugs Fixed in Errata RHSA-2009:0007

Along with the issues listed in *Section 1, "Important Changes for Red Hat Certificate System 7.3 Errata Update"*, these bugs were fixed in Certificate System 7.3 with Errata RHSA-2009:0007. The full list of Red Hat Certificate System erratas are available at *https://1rhn.redhat.com/1errata/1rhel-certserv-73-errata.html*.

Bug Number	Description
224732 249923 286941 452072 (CVE-2008-2367)	Several passwords were improperly written to plain text files, such as the subsystem debug log. These plain text files and other configuration files which had sensitive information did not have appropriate file permissions set to prevent unauthorized access to application passwords.
405451	End-entities pages for the different subsystem used Window's **xenroll.dll** for certificate enrollment, but this library was not supported in Windows Vista, so user could not request or enroll certificates through the end-entities pages using Microsoft Internet Explorer on Vista. These HTML interfaces have been updated to support the **certenroll.dll** library used on Vista.
426329 434567	The password used by the LDAP publisher was improperly stored in the CA configuration. This essentially required that the LDAP publishing password had to be the same as the internal database (LDAP directory) password, or LDAP publishing would break. A new parameter was added to the CA **CS.cfg** file to define an LDAP publishing password parameter in the CA's **password.conf** file.

Bug Number	Description
431470 433652 466188	The secure ports used by subsystem interfaces — the administrative console, agent pages, and end-entities pages — are, by default, the same. It is possible with this errata to run those services on separate port, which provides additional protection by prohibiting agents and users from accessing the same TCP port and web services directory.
452055	The certificate policies extension was not processed by CMSServlet.
459049	Any IP Address defined in a certificate's SubjectAltName parameter was improperly coded as an 8-byte number, with the last 4 bytes trailing zeros (**`00 00 00 00`**).
465879	The subject name uniqueness plug-in in the CA profiles, which enforces unique names for all active certificates, would reject a certificate request which reused a subject name even if the previous certificate had been revoked or expired.
473171 475998	The challenge-proof step for verifying the public key on the TPS behaved as if the verification had passed, even if the step had failed.
480100	The TPS dependences have been changed from MozLDAP5 to MozLDAP6.

Table 1. Fixed Bugs

4. Platform Support

This section contains information related to installing Red Hat Certificate System 7.3, including hardware and platform requirements and prerequisites.

4.1. Server Support

The Certificate System subsystems are supported on the following platforms:

- Red Hat Enterprise Linux AS 4 for i386
- Red Hat Enterprise Linux ES 4 for i386
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T
- 64-bit Solaris 9 for SPARC

4.1.1. Server Requirements

Component	Details
CPU	Intel — 2.0 GHz Pentium 4 or faster
RAM	1 GB (required)

Hard disk storage space	Total is approximately 5 GB
	• Total transient space required during installation: 1 GB
	• Hard disk storage space required for installation:
	  • Space required to set up, configure, and run the server: approximately 2 GB
	  • Additional space for database growth in pilot deployment: approximately 1 GB
	  • Total disk storage space for installation: approximately 1 GB

Table 2. Red Hat Enterprise Linux Server Requirements

4.1.2. Red Hat Enterprise Linux Considerations

Before installing the Certificate System packages, ensure that the proper dependencies are installed on the Red Hat Enterprise Linux system.

The following package groups and packages must be installed on all Red Hat Enterprise Linux systems:

- dialup (package group)
- gnome-desktop (package group)
- compat-arch-support (package group)
- web-server (package group)
- kernel-smp (package)

- e2fsprogs (package)
- firefox (package)

On 64-bit Red Hat Enterprise Linux platforms, ensure that the 64-bit (x86_64) **`compat-libstdc++`** libraries are installed, and not only the 32-bit (i386) libraries. To confirm this, run the following command as `root`:

```
rpm -qa --queryformat 'compat-libstdc++-%{VERSION}-%{RELEASE}.%{ARCH}.rpm
| grep x86_64
```

Numerous libraries should be displayed.

4.2. Client Support

The Enterprise Security Client is supported on the following platforms:

- Apple Macintosh OS X 10.4.x (Tiger) (Power PC, Intel)
- Microsoft Windows XP Professional (i386)
- Red Hat Enterprise Linux AS 4 (i386)
- Red Hat Enterprise Linux ES 4 (i386)
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T

4.3. Other Required Software

- *Red Hat Directory Server 7.1.*

  The source code and binaries for this component are available at *https://1rhn.redhat.com*), through the Red Hat Directory Server 7.1 channel.

- *Web browser software that supports SSL.*

  It is strongly recommended that users such as agents or administrators use Mozilla Firefox. End-entities should use Mozilla Firefox or Microsoft Internet Explorer.

  The only browser that is fully-supported for the HTML-based instance configuration wizard is Mozilla

Firefox.

Internet Explorer is supported on both Windows XP and Windows Vista.

4.4. Optional Server Hardware

Red Hat Certificate System supports Chrysalis-ITS LunaSA Hardware Security Module (HSM).

Architecture	Version
Firmware	4.5.2
Appliance Software	3.2.4
Client Software	3.2.4

4.5. Optional Client Hardware

- Axalto Global Platform compatible Cyberflex eGate token

5. Installation and Deployment Notes

The following sections contain important installation, configuration, and deployment information for Red Hat Certificate System 7.3.

5.1. Obtaining Packages

Red Hat Network (*http://1rhn.redhat.com*) is the software distribution mechanism for most Red Hat customers. Account login information for Red Hat Network, including entitlements for the Red Hat Certificate System 7.3 release, is required to download this software from Red Hat Network. After logging into Red Hat Network, go to the appropriate Red Hat Certificate System 7.3 channel to download the packages for the selected Red Hat Enterprise Linux platform.

NOTE

The source code for Red Hat Directory Server 7.1 is included with the ISO image downloaded for the 32-bit Red Hat Enterprise Linux version. Red Hat Certificate System 7.3 is not open source.

Red Hat Enterprise Linux systems can upgrade or download Red Hat Certificate System using **`up2date`**.

5.2. Installation Notes

- Packages are non-relocatable. The Red Hat Certificate System base packages can not be installed to a user-designated location.

- Do not use the Autorun feature of the CD drive. If you use the Autorun feature with a CD created from the ISO image, all subsystems (CA, DRM, OCSP, TKS, and TPS) as well as the Enterprise Security Client are installed on the system by default.

  The preferred alternative is to run the installation scripts provided for the server, or to follow the installation instructions in the *Red Hat Certificate System 7.3 Administration Guide*.

- Ensure that you remove any existing installations of *sqlite* RPM files for RA, specifically **`libsqlite`**. The **`sqlite-<XX>`** RPM files that ship with RA will cause conflicts with those files.

5.3. Required JRE

Java™ 1.5.0 Java Runtime Environment (JRE). Certificate System does not support earlier versions of the JRE. This JRE is required for running Tomcat, among other applications for the Certificate System.

On 32-bit Red Hat Enterprise Linux 4 platforms, Certificate System 7.3 requires the 32-bit version of the IBM JRE 1.5.0. A pre-packaged binary distribution of this package, the **`java-1.5.0-ibm`** rpm package, is available through either the **Red Hat Enterprise Linux AS (v. 4 for x86) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for x86) Extras** Red Hat Network channel.

A similar package is available for 64-bit Red Hat Enterprise Linux 4 platforms. This package is available through either the **Red Hat Enterprise Linux AS (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel.

As `root`, run **`/usr/sbin/alternatives --config java`** to ensure that the IBM Java™ 1.5.0 JRE is selected.

Warning

Both the 32-bit xSeries (Intel-compatible) and 64-bit AMD/Opteron/EM64T versions of the IBM J2SE JRE 5.0 RPM packages available through the IBM download site are packaged in a format which is incompatible with Certificate System 7.3.

5.4. Required JDK

A JDK must be present on Red Hat Enterprise Linux systems. See *http://kbase.redhat.com/faq/FAQ_54_4667.shtm* for more information. While almost any JDK is sufficient, installing one of these JDKs is recommended:

- For 32-bit Red Hat Enterprise Linux 4 platforms, a pre-packaged binary distribution of the 32-bit version of the IBM JDK 1.5.0, the **`java-1.5.0-ibm-devel`** rpm package, is available through either

the **Red Hat Enterprise Linux AS (v. 4 for x86) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for x86) Extras** Red Hat Network channel.

- A similar package is available for 64-bit Red Hat Enterprise Linux 4 platforms. This package is available through either the **Red Hat Enterprise Linux AS (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel.

After installing the JDK, run **`/usr/sbin/alternatives --config javac`** as `root` to ensure that a JDK is available.

5.5. TPS Subsystem Considerations

- TPS subsystems installed on a Red Hat Enterprise Linux system require a local installation of the Apache 2.0.x web server.

- The TPS subsystem cannot be cloned.

5.6. Directory Server Information

All subsystems require access to Red Hat Directory Server 7.1 on either the local machine (if it is also a 32-bit Red Hat Enterprise Linux platform) or a remote machine (acceptable platforms are 32-bit Red Hat Enterprise Linux 4, 32-bit Solaris 9 for SPARC, or 64-bit Solaris 9 for SPARC).

5.7. Source RPMs

Red Hat Certificate System 7.3 is not an open-source product. Consequently, source RPMs are only available for third-party packages.

NOTE

Several of these third-party packages may issue warnings when they are installed because they may contain the UID and GID of their original packager.

6. Copyright and Third-Party Acknowledgments

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.3 servers include the following:

Apache Software Foundation

Red Hat Certificate System TPS subsystems require a locally-installed Apache 2.0.x HTTP server. Although a local copy of this server is generally installed as part of the operating system (with its

corresponding license located in **/usr/share/doc/***httpd-version***/LICENSE**, the latest version of this server is available at the following URL:

http://httpd.apache.org

Red Hat Certificate System CA, DRM, OCSP, and TKS subsystems use a locally-installed Tomcat 5.5 web server. Although an appropriate server is installed when any of these subsystems are installed, the latest version of this server is available at the following URL:

http://tomcat.apache.org

Red Hat Certificate System uses many components made available from Apache.

- The XML project jars are **crimson.jar** and **xalan.jar**. These are available at the following URL:

  http://xml.apache.org [1]

- The Tomcat project jar files are **servlet.jar** and **jakarta-naming.jar**. These are available at the following URL:

  http://jakarta.apache.org/tomcat/index.html [2]

Mozilla Foundation

Red Hat Certificate System uses version 4.2 of the Java™ Security Services (JSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of and, potentially, the binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/security/pki/jss/index.html [3]

Red Hat Certificate System also uses version 4.6 of the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/nspr/index.html [4]

Additionally, Red Hat Certificate System uses version 3.11 of the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/security/pki/nss/index.html

Red Hat Certificate System includes a set of compiled binaries (from NSS 3.11) of several tools from the Mozilla Project provided for the convenience of the user. This includes **certutil**, **cmsutil**, **modutil**, **pk12util**, **signtool**, **signver**, and **ssltap**. If any problems are found in these specific tools, the source code and build instructions for the latest version of this tool and, potentially, a binary image for other newer tools are available at the following URL:

1 http://xml.apache.org
2 http://jakarta.apache.org/tomcat/index.html
3 http://www.mozilla.org/projects/security/pki/jss/index.html
4 http://www.mozilla.org/projects/nspr/index.html

http://www.mozilla.org/projects/security/pki/nss/tools/index.html [5]

Red Hat Certificate System includes version 1.5 R3 of Rhino JavaScript for Java™. If any problems are found in this specific distribution, the source code and build instructions for the latest version and, potentially, a binary image are available at the following URL:

http://www.mozilla.org/rhino/index.html [6]

Red Hat

Red Hat Certificate System requires a complete Red Hat Directory Server 7.1 binary, and the open source portion of Certificate System is available at the following URL:

https://1rhn.redhat.com

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.3 clients include the following:

Mozilla Foundation

USE AND AVAILABILITY OF OPEN SOURCE CODE. Portions of the Product were created using source code governed by the Mozilla Public License (MPL). The source code for the portions of the Product governed by the MPL is available from *http://www.mozilla.org* under those licenses.

Red Hat Enterprise Security Client uses the latest version of the XULRunner cross-platform package. XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. If any problems are found in this specific distribution, the source code and build instructions for the latest versions and, potentially, a binary image are available at the following URL:

http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes [7]

Red Hat Enterprise Security Client also uses the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/nspr/index.html [8]

Red Hat Enterprise Security Client also uses the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/security/pki/nss/index.html

Additional Red Hat Enterprise Security Client smart card libraries and modules:

- e-gate Smart Card Drivers for Windows 2000/XP Copyright 2002-2003 Schlumberger. All rights re-

5 http://www.mozilla.org/projects/security/pki/nss/tools/index.html
6 http://www.mozilla.org/rhino/index.html
7 http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes
8 http://www.mozilla.org/projects/nspr/index.html

served.

- e-gate Smart Card Driver for Mac OS X Copyright 2003 by Chaskiel Grundman.

  Copyright 2003 by Philip Edelbrock.

  Significantly based on the Alladin etoken driver (the T=1 code is not needed): Copyright 2002 by Andreas Jellinghaus.

  Copyright 2002 by Olaf Kirch.

  See license terms below for rights on both parts.

  Some header files are from the pcsclite distribution: Copyright 1999 David Corcoran.

- MUSCLE smart card middleware and applets

  Copyright 1999-2002 David Corcoran.

  Copyright 2002 Schlumberger Network Solution.

  All rights reserved.

The following license terms govern the identified modules and libraries:

- e-gate Smart Card Drivers for Windows 2000/XP:

  Limited Warranty/ Exclusive Remedies. Schlumberger warrants to the benefit of Customer only, for a term of sixty (60) days from the date of acquisition of the e-gate Smart Card ("Warranty Term"), that if operated as directed under normal use and service, the Software will substantially perform the functions described in its applicable documentation. Schlumberger does not warrant that the Software will meet Customer's requirements or will operate in combinations that Customer may select for use, or that the operation of the Software will be uninterrupted or error-free, or that all Software errors will be corrected. Schlumberger's sole obligation and liability under this limited warranty shall be, at Schlumberger's option, to remedy any substantial non-performance of the Software to the functional descriptions set forth in its applicable documentation. If Schlumberger is unable to satisfy the foregoing limited warranty obligations during the Warranty Term, then Schlumberger shall, upon Customer's written request for termination of this Agreement, refund to Customer all sums paid to Schlumberger for the licensing of the Software hereunder. These are Customer's sole and exclusive remedies for any breach of warranty.

  WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 5 ABOVE, THE SOFTWARE IS PROVIDED AS IS. SCHLUMBERGER AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES. TO THE EXTENT AUTHORIZED BY APPLICABLE LAW, ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, ARE SPECIFICALLY DISCLAIMED. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT.

  Limitation of Liability. Schlumberger's cumulative liability to Customer, or any third party, for loss or damages resulting from any claim, demand or action arising out of or relating to this Agreement or

use of the Software ("Damages"), shall not exceed the net amount paid to Schlumberger for the licensing of the Software, in this case, the cost of the single e-gate Smart Card. In no event shall Schlumberger or any Supplier be liable for any indirect, incidental, special consequential or exemplary damages of any character, including, without limitation, damages for lost profits, goodwill, work stoppage, computer failure and all other commercial damages.

- e-gate Smart Card Driver for Mac OS X:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

  - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

  - The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- MUSCLE smart card middleware and applets:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

  2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

  3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED

WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.